RECEIPT-FREE ELECTRONIC BETTING SYSTEM

Patent number: JP8315053
Publication date: 1996-11-29
Inventor: SAKO KAZUE; JIYOSEFU JIYON KIRIAN
Applicant: NEC CORP
Classification:
- international: G06F19/00; G07C13/00; G09C1/00; G09C1/00; H04L9/32
- european:
Application number: JP19960027775 19960215
Priority number(s):

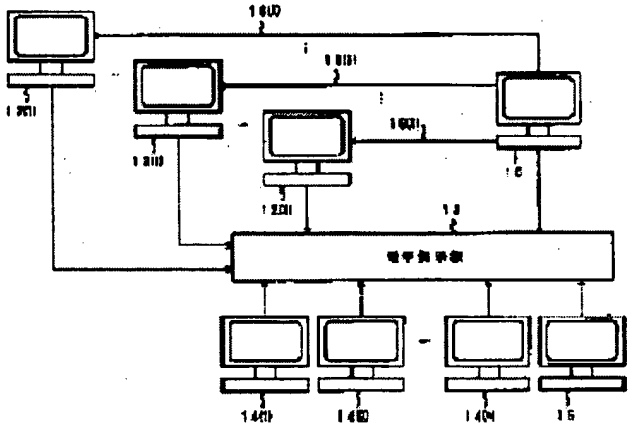
Also published as:
EP0743620 (A2)
US6092051 (A1)
EP0743620 (A3)
CA2176990 (C)
AU702945 (B2)

Report a data error here

Abstract of **JP8315053**

PURPOSE: To provide a safe receipt-free betting system by using algorithm based upon number theory.

CONSTITUTION: A bet generating center 10 generates a betting choice to each better or each bet selecting means 12. Ciphering or shuffling is applied to a bet and the result of ciphering and shuffling is sent to the bet selecting means 12 together with information on the method of applying shuffling to the bet without being intercepted on the way. The information is preferably transmitted through a safe tapping-disabled channel 16(i). Bet generation and shuffling verification using chameleon commitment and mutual communication proof can also be applied to this system. Thereby the betting system can be attained by using the tapping-disabled channel and a current personal computer provided with an access means to an electronic bulletin board.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平8－315053

(43)公開日　平成８年(1996)11月29日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　19/00			Ｇ０６Ｆ　15/28	Ｂ	
Ｇ０７Ｃ　13/00			Ｇ０７Ｃ　13/00	Ｂ	
Ｇ０９Ｃ　1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６４０Ｃ	
	６６０	7259－5Ｊ		６６０Ｚ	
Ｈ０４Ｌ　9/32		8842－5Ｊ	Ｈ０４Ｌ　9/00	６７５Ｃ	

審査請求　有　請求項の数40　ＯＬ　外国語出願　（全 35 頁）

(21)出願番号　特願平8－27775

(22)出願日　平成８年(1996)２月15日

(31)優先権主張番号　０８／４４４７０１

(32)優先日　1995年５月19日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　ジョセフ　ジョン　キリアン
アメリカ合衆国，ニュージャージー　08550，プリンストン　ジャンクション，リード　ドライヴ　ノース　18

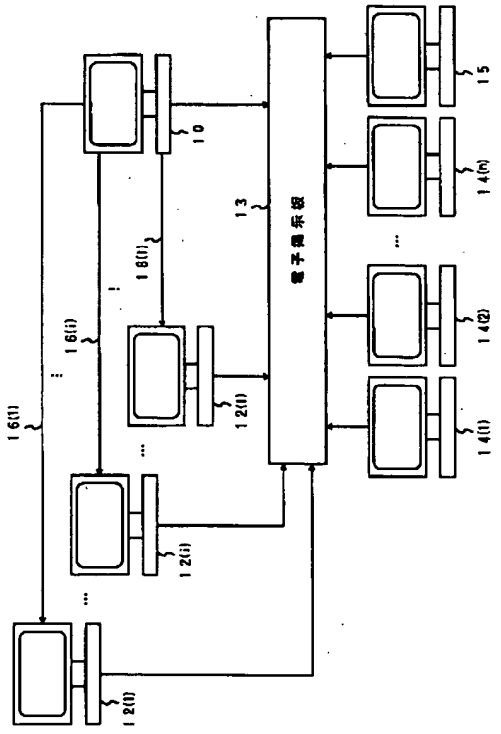
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　レシートフリー電子投票方式

(57)【要約】

【課題】　整数論に基づくアルゴリズムを用いて安全なレシートフリー投票方式を提供する。

【解決手段】　投票生成センター１０は、各投票者または各投票選択手段１２（ｉ）に対して投票の選択肢を生成する。投票は、暗号化およびシャッフリングを施され、投票がどのようにシャッフルされたかに関する情報とともに、途中で傍受されることなく、投票選択手段に送られる。この情報は、好ましくは、安全な盗聴不可能なチャンネル１６（ｉ）を通じて送られる。本方式に、カメレオンコミットメントおよび相互通信プルーフを用いた、投票生成およびシャッフリングの検証を組み入れることもできる。本発明は、盗聴不可能なチャンネルと電子掲示板１３へのアクセスを備えた現世代のパーソナルコンピューターにより実現できる。



1

【特許請求の範囲】

【請求項1】　(a) 各投票選択手段のための投票を構成して掲示板上に掲示するステップと、

(b) 傍受されることなく各投票選択手段に専用メッセージを送るステップと、

(c) 投票選択手段が投票を選択しメッセージを構成するステップと、

(d) 上記投票選択手段からのメッセージを安全な匿名チャンネルを介して投票集計センターに送達するステップと、

(e) 上記投票集計センターが投票を集計するステップとを含むことを特徴とする、安全なレシートフリー投票方式。

【請求項2】　上記専用メッセージを送るステップは、盗聴不可能な安全なチャンネルを介して送るものであることを特徴とする、請求項1に記載の安全なレシートフリー投票方式。

【請求項3】　投票構成の正当性を証明するステップをさらに含むことを特徴とする、請求項1に記載の安全なレシートフリー投票方式。

【請求項4】　上記正当性を証明するステップは、1－0証明アルゴリズムを実行することにより行なわれることを特徴とする、請求項3に記載の安全なレシートフリー投票方式。

【請求項5】　(f) 上記投票を構成するステップであって、カメレオン・コミットメントを用いてランダムストリングをコミットすることを含むステップと、

(g) コミットされたビットを用いることにより構成された投票の正当性を証明するステップと、

(h) 盗聴不可能な安全なチャンネルを介してデコミットするステップとをさらに含むことを特徴とする、請求項3に記載の安全なレシートフリー投票方式。

【請求項6】　上記正当性を証明するステップは、1－0証明アルゴリズムを実行することにより行なわれることを特徴とする、請求項5に記載の安全なレシートフリー投票方式。

【請求項7】　上記投票選択手段が上記カメレオン・コミットメントを無効化するステップをさらに含むことを特徴とする、請求項5に記載の安全なレシートフリー投票方式。

【請求項8】　上記正当性を証明するステップは、1－0証明アルゴリズムを実行することにより行なわれることを特徴とする、請求項7に記載の安全なレシートフリー投票方式。

【請求項9】　上記投票選択手段が上記カメレオン・コミットメントを無効化するステップは、投票を構成するための秘密鍵を上記掲示板に与えるものであることを特徴とする、請求項7に記載の安全なレシートフリー投票方式。

【請求項10】　上記ステップ (a) は、

2

(i) 上記構成された投票をシャッフルすること、および、

(ii) 上記シャッフリングに関する専用メッセージを、傍受されることなく、上記投票選択手段に送ることをさらに含むことを特徴とする、請求項1に記載の安全なレシートフリー投票方式。

【請求項11】　上記専用メッセージを送るステップは、盗聴不可能な安全なチャンネルを介して送るものであることを特徴とする、請求項10に記載の安全なレシートフリー投票方式。

【請求項12】　上記ステップ (a) は、

(i) 上記構成された投票をシャッフルすること、および、

(ii) 上記シャッフリングに関する専用メッセージを、傍受されることなく、上記投票選択手段に送ることをさらに含むことを特徴とする、請求項2に記載の安全なレシートフリー投票方式。

【請求項13】　上記専用メッセージを送るステップは、盗聴不可能な安全なチャンネルを介して送るものであることを特徴とする、請求項4に記載の安全なレシートフリー投票方式。

【請求項14】　上記ステップ (a) は、

(i) 上記構成された投票をシャッフルすること、および、

(ii) 上記シャッフリングに関する専用メッセージを、傍受されることなく、上記投票選択手段に送ることをさらに含むことを特徴とする、請求項5に記載の安全なレシートフリー投票方式。

【請求項15】　上記専用メッセージを送るステップは、盗聴不可能な安全なチャンネルを介して送るものであることを特徴とする、請求項14に記載の安全なレシートフリー投票方式。

【請求項16】　上記ステップ (a) は、

(i) 上記構成された投票をシャッフルすること、および、

(ii) 上記シャッフリングに関する専用メッセージを、傍受されることなく、上記投票選択手段に送ることをさらに含むことを特徴とする、請求項7に記載の安全なレシートフリー投票方式。

【請求項17】　上記専用メッセージを送るステップは、盗聴不可能な安全なチャンネルを介して送るものであることを特徴とする、請求項16に記載の安全なレシートフリー投票方式。

【請求項18】　上記ステップ (a) は、

(i) 上記構成された投票をシャッフルすること、および、

(ii) 上記シャッフリングに関する専用メッセージを、傍受されることなく、上記投票選択手段に送ることをさらに含むことを特徴とする、請求項3に記載の安全なレシートフリー投票方式。

3

【請求項１９】　上記専用メッセージを送るステップは、盗聴不可能な安全なチャンネルを介して送るものであることを特徴とする、請求項１８に記載の安全なレシートフリー投票方式。

【請求項２０】　上記構成されシャッフルされた投票の正当性を証明するステップをさらに含むことを特徴とする、請求項１０に記載の安全なレシートフリー投票方式。

【請求項２１】　（ｆ）カメレオン・コミットメントを用いてランダムストリングをコミットするステップと、

（ｇ）コミットされたビットを用いることにより上記構成されシャッフルされた投票の正当性を証明するステップと、

（ｈ）傍受されることなくデコミットするステップとをさらに含むことを特徴とする、請求項２０に記載の安全なレシートフリー投票方式。

【請求項２２】　上記デコミットするステップは、盗聴不可能な安全なチャンネルを介して行なわれることを特徴とする、請求項２１に記載の安全なレシートフリー投票方式。

【請求項２３】　上記正当性を証明するステップは、証明シャッフルアルゴリズムを実行することにより行なわれることを特徴とする、請求項２０に記載の安全なレシートフリー投票方式。

【請求項２４】　上記正当性を証明するステップは、証明シャッフルアルゴリズムを実行することにより行なわれることを特徴とする、請求項２１に記載の安全なレシートフリー投票方式。

【請求項２５】　カメレオン・コミットメントを無効化するステップをさらに含むことを特徴とする、請求項２１に記載の安全なレシートフリー投票方式。

【請求項２６】　カメレオン・コミットメントを無効化するステップをさらに含むことを特徴とする、請求項２３に記載の安全なレシートフリー投票方式。

【請求項２７】　上記カメレオン・コミットメントを無効化するステップは、上記シャッフリングのための秘密鍵を上記掲示板に与えることを含むことを特徴とする、請求項２６に記載の安全なレシートフリー投票方式。

【請求項２８】　複数の投票生成センターと、

複数の投票選択手段と、

掲示板と、

投票集計センターとを備え、

上記投票生成センターは、上記投票者の各々のための投票を構成して上記掲示板上に掲示し、さらに、上記投票生成センターは、傍受されることなく各投票選択手段に専用メッセージを送り、

上記投票選択手段の各々は、投票を選択するとともに、安全な匿名チャンネルを介して上記投票集計センターに送達されるメッセージを構成し、

上記投票集計センターは投票を集計することを特徴とする、安全なレシートフリー投票装置。

4

【請求項２９】　上記投票生成センターは、盗聴不可能な安全なチャンネルを介して、上記専用メッセージを上記投票選択手段に送ることを特徴とする、請求項２８に記載の安全なレシートフリー投票装置。

【請求項３０】　上記投票生成センターは、カメレオン・コミットメントを用いてランダムストリングをコミットし、コミットされたビットを用いて投票構成の正当性を証明し、盗聴不可能な安全なチャンネルを介してデコミットするステップをさらに行なうことを特徴とする、請求項２８に記載の安全なレシートフリー投票装置。

【請求項３１】　上記投票選択手段は、カメレオン・コミットメントを無効化するステップをさらに行なうことを特徴とする、請求項３０に記載の安全なレシートフリー投票装置。

【請求項３２】　上記構成された投票を受けとるためのシャッフリングセンターのシャッフルネットをさらに備え、

上記シャッフルネット内の各シャッフリングセンターは、投票をシャッフルし、傍受されることなく投票選択手段に専用メッセージを送ることを特徴とする、請求項２８に記載の安全なレシートフリー投票装置。

【請求項３３】　各シャッフリングセンターは、盗聴不可能な安全なチャンネルを介して、上記専用メッセージを上記投票選択手段に送ることを特徴とする、請求項３２に記載の安全なレシートフリー投票装置。

【請求項３４】　上記構成された投票を受けとるためのシャッフリングセンターのシャッフルネットをさらに備え、

上記シャッフルネット内の各シャッフリングセンターは、投票をシャッフルし、傍受されることなく上記投票選択手段に上記専用メッセージを送ることを特徴とする、請求項３０に記載の安全なレシートフリー投票装置。

【請求項３５】　各シャッフリングセンターは、盗聴不可能な安全なチャンネルを介して、上記専用メッセージを上記投票選択手段に送ることを特徴とする、請求項３４に記載の安全なレシートフリー投票装置。

【請求項３６】　上記シャッフリングセンターは、さらに、投票構成の正当性を証明するステップを行なうことを特徴とする、請求項３２に記載の安全なレシートフリー投票装置。

【請求項３７】　各シャッフリングセンターは、カメレオン・コミットメントを用いてランダムストリングをコミットし、コミットされたビットを用いて投票構成の正当性を証明し、傍受されることなくデコミットするステップをさらに行なうことを特徴とする、請求項３６に記載の安全なレシートフリー投票装置。

【請求項３８】　上記デコミットするステップは、盗聴不可能な安全なチャンネルを介して行なわれることを特

5

徴とする、請求項３７に記載の安全なレシートフリー投票装置。

【請求項３９】　各投票選択手段が、カメレオン・コミットメントを無効化するステップをさらに行なうことを特徴とする、請求項３７に記載の安全なレシートフリー投票装置。

【請求項４０】　各投票選択手段は、その秘密鍵を上記シャッフリングセンターにまたは上記掲示板に与えることによりカメレオン・コミットメントを無効化することを特徴とする、請求項３９に記載の安全なレシートフリー投票装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、安全なレシートフリー電子投票に有用な方式および装置に関し、特に、安全なレシートフリー電子投票のための、整数論に基づくアルゴリズムに関する。

【０００２】

【従来の技術】安全な電子投票の最終目標は、物理的投票ブースにとって代わることである。この目標を達成するには、現在のプロトコルの効率の改善、ならびに、これらの物理的装置が提供できる秘密保持特性の理解の双方についての研究が要求される。

【０００３】最近では、ＳＴＯＣ９４（１９９４年発行）の５４４～５５３頁に掲載された「Ｒｅｃｅｉｐｔ－ｆｒｅｅ　Ｓｅｃｒｅｔ－ｂａｌｌｏｔ　Ｅｌｅｃｔｉｏｎ（レシートフリー秘密投票選挙）」と題するＪ．Ｃ．Ｂｅｎａｌｏｈらの論文に、物理的投票プロトコルとは異なり、ほとんどすべての電子投票プロトコルにおいては、どのように投票したかを証する受領書を投票者に与えていることが示されている。このような受領書は、投票者が投票を売ったり、別の者が投票者に投票の仕方を強制したりすることのできる容易な手段となってしまう。

【０００４】ＢｅｎａｌｏａおよびＴｕｉｎｓｔｒａは、第１のレシートフリー電子投票プロトコルを提案している。彼らの方法によれば、委託センターが、各投票者に対し、ランダムな配列の「賛成」票および「反対」票からなる一対の投票券を発行する。確実なビーコンおよび物理的投票ブースを用いて、センターは、投票券が実際に正しく構成された「賛成／反対」または「反対／賛成」対であることを公衆に証明し、同時に、検証者に対しそれがどちらの対であるかを証明する。物理的装置により、検証者は、部外者と通信できる時点までに、投票券が「賛成／反対」であることのプルーフを偽造したり、「反対／賛成」であることのプルーフを偽造したりすることができる。このようなプルーフは、もはや、受領書としていずれの証拠にもなることはない。

【０００５】これとは別に、ＮｉｅｍｉおよびＲｅｎｖａｌｌは、ＡＳＩＡＣＲＹＰＴ´９４（１９９４年発行）の１４１～１４８頁に掲載された「Ｈｏｗ　ｔｏ　ｐｒｅｖｅｎｔ　ｂｕｙｉｎｇ　ｏｆ　ｖｏｔｅｓ　ｉｎ　ｃｏｍｐｕｔｅｒ　ｅｌｅｃｔｉｏｎｓ（コンピュータ選挙において投票の買収を防ぐ方法）」と題するＮｉｅｍｉらの論文において、この問題を解決しようとしている。彼らも物理的投票ブースを用い、投票者はここですべてのセンターとマルチパーティ計算を行なう。

6

【０００６】

【発明が解決しようとする課題】Ｂｅｎａｌｏｈ－ＴｕｉｎｓｔｒａおよびＮｉｅｍｉ－Ｒｅｎｖａｌｌのプロトコルの両方とも、安全なレシートフリー投票が可能であることを示している。しかしながら、その物理的要件はかなりめんどうなものであり、物理的選挙において参加者が直面するものとは異なっている。重要な未解決の課題は、安全なレシートフリー投票を達成するためには厳密にどんな物理的要件が必要であるかということである。

【０００７】

【課題を解決するための手段】本発明によれば、より実用的な物理的要件、すなわち、物理的に安全な盗聴不可能な専用チャンネルを備えた、安全なレシートフリー投票方式が得られる。

【０００８】本発明による安全なレシートフリー投票方式においては、物理的に安全な盗聴不可能なチャンネルを用いることにより、各投票者は、どのように投票したかの証拠を残さない。「盗聴不可能な安全なチャンネル」なる用語は、他者にアクセスすなわち検出されることなくセンターからメッセージを送り得ることを言う。このような盗聴不可能なチャンネルは、１９９２年１０月発行のＳｃｉｅｎｔｉｆｉｃ　Ａｍｅｒｉｃａｎ、第２６７巻第４号、５０～５７頁に掲載された「Ｑｕａｎｔｕｍ　Ｃｒｙｐｔｏｇｒａｐｈｙ（量子暗号法）」と題するＣ．Ｂｅｎｎｅｔｔらの論文に記載されている。盗聴不可能なチャンネルを用いることの最終結果は、投票者も他者も、どんな票を入れたかあるいはどんなメッセージを送ったかを見せたり証明したりできないことである。いったんメッセージを送るか受けとるかすると、内容は変更されメッセージのプルーフを不可能にする。しかしながら、メッセージが途中であるいは受領時に傍受すなわち検出された場合には、傍受すなわち検出した者は、変更が可能となる時点より前にメッセージの内容を知ることができる。さらに、たとえ安全でないチャンネルを用いたとしても、メッセージが傍受すなわち検出されることなくチャンネルに沿って進行した場合には、本発明に用いられるプロトコルにより、いったんその送付先において受領した後では、その票がどんな票であったかの判定は可能ではない。言い換えれば、盗聴不可能なチャンネルとは、途中で傍受すなわち検出されることなくメッセージを伝達することをいう。

【０００９】以下の説明において、「カメレオン・コミ

ットメント」なる用語が用いられる。カメレオン・コミットメントは、メッセージをコミット（封印）およびデコミット（開封）するプロトコルであり、コミッターはコミッターがコミットしたとおりデコミットでき、一方、受取人はコミッターがどのようにコミットしたかにかかわらずどのようにもデコミットできる。

【００１０】本発明の方式によれば、投票生成センターと、投票集計センターと、種々のセンターと各投票者との間でメッセージを転送するためのシャッフリングセンターが設けられる。本発明の方式は以下の３つのステップからなる。

【００１１】第１のステップは、投票生成センターが、各投票者に対して、ひと組のあらゆる可能な投票を発行することである。ここでは、簡略化のために、可能な投票は２種類、すなわち、「1」票と「0」票であると仮定する。各投票者ｉに対して、投票生成センターは、ランダムな配列の暗号化された「1」票と「0」票を与える。コミッターはカメレオン・ビット・コミットメントを用いて配列に対してコミットする。センターは、コミッターが投票対を正しく構成したことを証明する。コミッターは、盗聴不可能な安全なチャンネルを介してその投票者のみに配列をデコミットする。

【００１２】第２のステップは、投票生成センターからシャッフリングセンターを介して、投票者に投票を転送することである。各シャッフリングセンターは、シャッフルネットを介して投票者ｉに対する２つの投票をシャッフルする。コミッターは、カメレオン・コミットメントを用いて、どのように投票をシャッフルするかに関してコミットする。各シャッフリングセンターは、その動作の正当性を証明する。コミッターは、盗聴不可能な安全なチャンネルを介して、投票者ｉに対してのみ、どのように投票がシャッフルされたかを通知する。

【００１３】第２のステップは必須のものではなく、省略する場合には、投票生成センターは、通常のチャンネルを介して投票者に直接、投票を送る。

【００１４】第３のステップは投票者による匿名投票である。投票対の最初の配列様式と、第２のステップにおいてそれらがどのようにシャッフルされたかを保存しておくことにより、各投票者にはどちらの票がどれであるかがわかる。各投票者は受領した投票のうちの１つを、安全な匿名チャンネルを介して集計センターに提出する。つぎに、集計センターは投票数を計算する。

【００１５】安全な匿名チャンネルの実現は、１９９３年発行のＡｄｖａｎｃｅｓ　ｉｎＣｒｙｐｔｏｌｏｇｙ，　Ｅｕｒｏｃｒｙｐｔ　’９３の２４８～２５９頁に掲載された「Ｅｆｆｉｃｉｅｎｔ　Ａｎｏｎｙｍｏｕｓ　Ｃｈａｎｎｅｌ　ａｎｄＡｌｌ／Ｎｏｔｈｉｎｇ　Ｅｌｅｃｔｉｏｎ　Ｓｃｈｅｍｅ（効率的な匿名チャンネルおよびオール・オア・ナッシング投票方式）」と題するＣ．Ｐａｒｋらの論文や、本発明と同一の譲受人に譲渡された「Ｓｅｃｕｒｅ　Ａｎｏｎｙｍｏｕｓ　Ｍｅｓｓａｇｅ　Ｔｒａｎｓｆｅｒ　ａｎｄ　Ｖｏｔｉｎｇ　Ｓｃｈｅｍｅ（安全な匿名メッセージ転送および投票方式）」と題する米国特許出願第０８／３７６，５６８号に示されている。また、本発明によれば、多数のプルーフを単一プルーフに合成することによりプルーフの作成、伝送、チェックに必要な通信量および計算量を削減した方法が得られる。

【００１６】

【発明の実施の形態】以下、本発明を、添付図面を用いて詳細に説明する。

【００１７】本発明の好ましい実施の形態による安全なレシートフリー投票方式を図１および図２を参照して説明する。本発明の方式によれば、投票構成プロセス２６により投票生成センター１０が生成した暗号化投票は、電子掲示板１３その他の公衆アクセス可能な報知手段上に送付される。暗号化投票は、各投票選択手段１２（ｉ）に対して、ランダムな配列に並べ変えた「1」票と「0」票の対からなる。つぎに投票生成センター１０は、投票選択手段１２（ｉ）に対する暗号化投票がどのように配列されているかを、盗聴不可能なチャンネル１６（ｉ）を介して、投票選択手段１２（ｉ）に秘密に伝達する。同時に、投票生成センター１０は、公衆に対しては、投票が公正に生成されたことを、投票選択手段に対しては、センター１０が秘密メッセージ中に誤った情報を送らなかったことを、それぞれ証明する必要がある。これらの証明は、後述するように、次の証明プロセス２０により実行される。

【００１８】投票選択手段１２（ｉ）は、物理的に盗聴不可能なチャンネル１６（ｉ）を介して投票生成センター１０から送られる秘密メッセージを用いて、その票を選択する。投票選択手段１２（1）、１２（2）、…、１２（l）により選択された投票は、投票集計センター１５に、安全な匿名チャンネルを介して無記名で転送される。安全な匿名チャンネル１４は、ミキシングセンター１４（1）、１４（2）、…、１４（n）により実現される。すなわち、暗号化投票は、ミキシングセンターにより次々に処理され、投票集計センター１５が、ランダムにかつ追跡不能に配列した一組の非暗号化投票と計算結果とを出力するまで続けられる。投票生成センター１０、投票選択手段１２（ｉ）、ミキシングセンター１４（ｉ）、投票集計センター１５の各々は、計算手段、好ましくは、パーソナルコンピュータから構成されるが、ワークステーションその他でも差支えない。

【００１９】以上、本発明の方式の概略を説明したが、つぎに、投票構成プロセス２６と、証明プロセス２０と、盗聴不可能なチャンネル１６を介して安全に転送される情報の詳細について説明する。

【００２０】投票生成センター１０は、投票構成プロセス２６を実行することにより、各投票選択手段１２

9

（i）に対して「0」票および「1」票からなる暗号化対を生成する。センターは、独立して選択された乱数を用いて、各投票選択手段12（i）に対する投票構成プロセスを行なう。

【0021】「1」票と「0」票の暗号化形態は、匿名チャンネルに入力するのに適したものでなければならな*

$$v_{i}^{0} = (g^{r_{i1}} \bmod p,\ m_0 \cdot y^{r_{i1}} \bmod p)$$
$$v_{i}^{1} = (g^{r_{i2}} \bmod p,\ m_1 \cdot y^{r_{i2}} \bmod p) \quad (1)$$

ここでr_{i1}およびr_{i2}は投票選択手段12（i）に対する独立乱数であり、p，g，y，m_0、m_1はすべての投票選択手段に対して適当に選択された共通定数である。投票構成プロセス26は、ランダムに選択された乱数r_{i1}およびr_{i2}を用いて上式を計算することを含んでいる。

【0023】投票生成センター10は、2分の1の確率で（v_{i}^{0}，v_{i}^{1}）の順に、それ以外は（v_{i}^{1}，v_{i}^{0}）の順に、掲示板上に掲示する。

【0024】証明プロセス20は、3つのアルゴリズムから構成される。すなわち、コミットメントアルゴリズム21、1－0証明アルゴリズム22、デコミットメントアルゴリズム23である。コミットメントアルゴリズム21は、上記配列についてのカメレオン・コミットメントと、つぎの1－0証明プロトコルに用いられるランダムシーケンスを計算して掲示するために用いられる。1－0証明アルゴリズムは、複数回実行され、投票生成センター10が公正に投票を生成し、その出力が電子掲示板13上に掲示されていることを証明する。デコミットメントアルゴリズム23は、盗聴不可能な安全なチャンネルを介して、コミットメントアルゴリズム21においてコミットされたカメレオン・コミットメントをデコミットするために用いられる。1－0証明およびカメレオン・コミットメント／デコミットメントのアルゴリズムについては後述する。

【0025】投票生成センターは、カメレオン・デコミットメントである、デコミッターの出力を、盗聴不可能なチャンネルを介して投票選択手段12（i）に送る。

【0026】投票選択手段12（i）は、検証プロセス24により、1－0証明アルゴリズムの正当性と、デコミットメントの有効性を検証する。これらの正当性と有効性が検証されると、投票選択手段12（i）は、選択プロセス25を実行し、掲示板上の暗号化投票のうち、※

$$E_0(v^0) = (g^{r'} \bmod p,\ m_0 \cdot y^{r'} \bmod p)$$
$$E_1(v^1) = (g^{r'} \bmod p,\ m_1 \cdot y^{r'} \bmod p)$$

そして、コミットされたストリングにしたがった順序で$E_0(v^0)$および$E_1(v^1)$を送付する。

【0033】2a．1／2の確率をもって、証明手段は、r′およびr″を明らかにすることを要求される。検証手段は、$E_0(v^0)$および$E_1(v^1)$が矛盾することなく作成されているかどうかをチェックする。

【0034】2b．1／2の確率をもって、証明手段

10

*い。好ましくは、ここに参照として組み入れた米国特許出願第08／376，568号に記載された方法および装置を用い、「1」票と「0」票の暗号化形態をつぎのように選択する。

【0022】

※その意見をあらわす1つを選択する。投票選択手段には、暗号化投票がどのような配列であるかがカメレオン・デコミットメントからわかるので、正しい選択をすることができる。

【0027】投票選択手段12（i）により選択された投票は、他の投票選択手段により選択された他の投票とともに、シャッフルネットへの入力となる。

【0028】上述の方法を適用すると、悪意ある者が投票選択手段12（i）にその投票を開示することを強制しても、投票生成センター10が投票を開示することを許されないかぎり、あるいは、盗聴不可能なチャンネル16（i）が盗聴されないかぎり、選択された投票が「1」票であったか「0」票であったかの具体的なプルーフを受けとることはできない。

【0029】つぎに、1－0証明ならびにカメレオン・コミットメント／デコミットメントのアルゴリズムを説明する。1－0証明アルゴリズムは、証明手段と検証手段とを含む。この場合には、証明手段は投票生成センターである。検証手段は、投票選択手段を含め、いかなる実在でもよい。このアルゴリズムの確率挙動は、適当なハッシュ関数の出力により決定されるが、ランダムビーコンでもよい。

【0030】このアルゴリズムは、式（1）にしたがって生成され掲示された、ランダムに並べ変えた対（v_{i}^{0}，v_{i}^{1}）を受けて、それらが実際に「1」票と「0」票の対であると証明することを含んでいる。ここで、投票選択手段に対して、カメレオン・コミットメントを用いてランダムストリングがコミットされているものと仮定する。

【0031】1－0証明アルゴリズム

1．証明手段はr′、r″を一様に選択し、次の計算を行なう。

【0032】

$$E_0(v^0) = (g^{r'} \bmod p,\ m_0 \cdot y^{r'} \bmod p)$$
$$E_1(v^1) = (g^{r'} \bmod p,\ m_1 \cdot y^{r'} \bmod p)$$

は、$s_1 = r_{i1} - r'$および$s_2 = r_{i2} - r''$を明らかにすることを要求される。検証手段は、s_1、s_2、g、yを用いて$E_0(v^0)$および$E_1(v^1)$からv_{i}^{0}およびv_{i}^{1}を実際に生成できることをチェックする。

【0035】つぎにカメレオン・コミットメント法を説明する。カメレオン・コミットメント法は、送出部と受

領部を含む。送出部はこの場合には投票生成センターである。受領部は投票選択手段である。

【００３６】以下、ひとつのビットである０または１をコミットする場合に関して説明するが、複数ビットやストリングをコミットするように簡単に変形できることは言うまでもない。ここで、受領部は、公開整数αに対して$\alpha = g^a$を満足するａを知っているものとする。

【００３７】コミットメント：送出部は、受領部に対し、０をg^rにより、また、１に対しては$\alpha \cdot g^r$をコミットする。

【００３８】デコミットメント：送出部はｒを明らかにする。受領部は、g^rと$\alpha \cdot g^r$の両方を計算し、コミットメントされたビットは何であったかを決定する。

【００３９】デコミットメントを修正するために、受領部は、ｒではなくｒ－ａを受けとったと主張することができ、この場合は、送出部が他の値をコミットしたことになる。

【００４０】カメレオン・コミットメントのより詳細な説明は、１９８８年発行のＪＣＳＳ１５６～１８９頁に掲載された「Ｍｉｎｉｍｕｍ　Ｄｉｓｃｌｏｓｕｒｅ　Ｐｒｏｏｆｓ　ｏｆ　Ｋｎｏｗｌｅｄｇｅ（情報の最小開示プルーフ）」と題するＢｒａｓｓａｒｄ、Ｃｈａｕｍ、Ｃｒｅｐｅａｕの論文に記載されている。

【００４１】投票生成センターがそのランダムストリングをデコミットした後、投票選択手段１２（ｉ）は、無効化プロセス２７を行ない、センターのコミットメントを無効化する。無効化プロセス２７は、センターに値ａを通知し、センターに、後で誤った情報を提供する能力、または、値ａを掲示板１３上に掲示する能力をも持たせるようにすることを含んでいる。

【００４２】投票選択手段がコミットメントを修正する能力をもつこと、すなわち、投票選択手段が指数ａを知っていることを確実にするため、コミットメントを適用する前に、あるいは、投票の開始前でもよいが、投票生成センターと各投票選択手段の間に相互通信を起こさせてもよい。たとえば、投票選択手段がカットアンドチューズ（公平な分配）プロトコルを実行して定数αをえらべば、投票選択手段は高い確率でａを知ることになる。

【００４３】レシートフリー特性の安全性をより高めるため、図３および図４に示すように、多数のシャッフリングセンター１１（１）、１１（２）、…、１１（ｍ）からなるシャッフルネット１１を組み入れることができる。投票生成センター１０が投票選択手段１２（ｉ）に対して生成した各暗号化投票は、投票選択手段１２（ｉ）に達する前にシャッフルネット１１を通過する。＊

$$S(X_1) = (A_1 \cdot g^{c_1} \bmod p,\ A_2 \cdot y^{c_1} \bmod p)$$
$$S(X_2) = (B_1 \cdot g^{c_2} \bmod p,\ B_2 \cdot y^{c_2} \bmod p) \quad (2)$$

および、ランダムな順序でＳ（X_1）およびＳ（X_2）を送付することを含む。

【００５０】この順序および証明シャッフルアルゴリズムに用いられるランダムシーケンスは、カメレオン・コミットメントを用いてコミットされ、コミットメントアルゴリズム３２の出力として掲示板上に掲示される。

＊このような構成により、すべてのシャッフリングセンターおよび投票生成センターと共謀しないかぎり、あるいはシャッフリングセンターと投票選択手段１２（ｉ）間の盗聴不可能なチャンネル１７（１）、１７（２）、…、１７（ｍ）をすべて盗聴しないかぎり、悪意ある者が、投票選択手段１２（ｉ）がどのように投票したかを判定することはできない。

【００４４】各投票シャッフリングセンターは、計算手段、好ましくはパーソナルコンピュータから構成されるが、ワークステーションその他でも差支えない。

【００４５】シャッフルネットおよびシャッフリングセンターの動作について説明する。シャッフリングセンター１１（ｊ）は、前のシャッフリングセンター１１（ｊ－１）（ｊ＝１のとき、投票生成センター１０）により送付された各メッセージを処理し、配列を並べ変えたシャッフルプロセス３０（図５）の結果を送付する。これを、最後のシャッフリングセンター１１（ｍ）がシャッフリング結果を送付するまで続ける。各シャッフリングセンターは、投票がどのようにシャッフルされたかを、安全な盗聴不可能なチャンネル１７（ｊ）を介して投票選択手段に知らせる。各シャッフリングセンターは、投票生成センターと同様にして、公正にシャッフルしたことおよび誤った情報を与えなかったことを投票選択手段に対して証明する。これは証明プロセス３１により実行される。

【００４６】図５は、シャッフリングセンター１１（ｉ）の動作を示す。シャッフリングセンター１１（ｉ）は、シャッフルプロセス３０および証明プロセス３１を実行し、出力を送付する。証明プロセス３１は、投票選択手段に対するランダムストリングにカメレオンコミットメントを施すところのコミットメントアルゴリズム３２を含む。

【００４７】証明プロセス３１は、３つのアルゴリズム、すなわち、コミットメントアルゴリズム３２、証明シャッフルアルゴリズム３３、デコミットメントアルゴリズム３４を含む。

【００４８】シャッフルプロセス３０を説明するために、入力が、次のように表わされるシャッフル済み暗号化投票であると仮定する。

【００４９】$X_1 = (A_1, A_2)$
$X_2 = (B_1, B_2)$
シャッフルアルゴリズムは、乱数c_1およびc_2を発生すること、暗号化投票X_1およびX_2を次式のようにシャッフルすること、

13

【００５１】証明シャッフルアルゴリズム３３は、シャッフリングセンターがシャッフルアルゴリズムを正しく実行したことを証明するために用いられる。証明シャッフルアルゴリズムは、証明手段と検証手段を含む。この場合には、証明手段はシャッフリングセンターである。検証手段は、投票選択手段を含め、いかなる実在でもよい。このアルゴリズムの確率挙動は、適当なハッシュ関＊

$$E(X_1) = (A_1 \cdot g^{c'} \bmod p,\ A_2 \cdot y^{c'} \bmod p)$$

$$E(X_2) = (B_1 \cdot g^{c'} \bmod p,\ B_2 \cdot y^{c'} \bmod p)$$

そして、コミットされたストリングにしたがった順序でE（X_1）およびE（X_2）を送付する。

【００５４】２ａ．１／２の確率をもって、証明手段は、ｃ′およびｃ″を明らかにすることを要求される。検証手段は、E（X_1）およびE（X_2）が矛盾することなく作成されているかどうかをチェックする。

【００５５】２ｂ．１／２の確率をもって、証明手段は、$t_1 = c_1 - c'$および$t_2 = c_2 - c''$を明らかにすることを要求される。検証手段は、t_1、t_2、ｇ、ｙを用いてS（X_1）およびS（X_2）からE（X_1）およびE（X_2）を実際に生成できることをチェックする。

【００５６】投票生成センターにより送られた、暗号化投票は、シャッフリングセンター１１（１）、１１（２）、…、１１（ｍ）によりつぎつぎに処理され、最後のセンターが、ランダムかつ追跡不能に配列した一組の暗号化投票を出力して各投票選択手段に与えるまで続けられる。

【００５７】投票選択手段１２（ｉ）は、安全な盗聴不可能なチャンネル１６（ｉ）、１７（１）、１７（２）、…、１７（ｍ）を介して投票生成センターおよびシャッフリングセンターから受け取った秘密メッセージを用いて、投票を選択する。

【００５８】シャッフリングセンターのカメレオン・コミットメントの無効化は、投票生成センターのコミットメントの無効化と同様にして実現される。

【００５９】本発明を実施する好ましい方式を説明してきたが、つぎに、本発明を実施するために用いられる装置の好ましい実施形態を説明する。

【００６０】図１は、本発明の方式を実施するための装置の好ましい実施形態を概略的に示している。投票生成センター１０と、投票選択手段１２（１）、１２（２）、…、１２（ｌ）と、ミキシングセンター１４（１）、１４（２）、…、１４（ｎ）と、投票集計センター１５は、従来の電子掲示板１３に接続されたパーソナルコンピュータやワークステーションを用いている。安全な盗聴不可能なチャンネル１６（１）、１６（２）、…、１６（ｌ）を設けて、投票生成センターから各投票選択手段に秘密メッセージを送ることができるように構成されている。メッセージ転送プロセスを構成するすべての要素（送出部、検証手段、センターなど）

14

＊数の出力により決定されるが、ランダムビーコンでもよい。このアルゴリズムは、並べ変えられた（S（X_1），S（X_2））の対を含む。

【００５２】証明シャッフルアルゴリズム

１．証明手段はｃ′、ｃ″を一様に選択し、次の計算を行なう。

【００５３】

は、電子掲示板１３にメッセージを送付したりそこからメッセージを受けとったりすることにより相互に働きかける。ただし、投票生成センターが、盗聴不可能なチャンネルを介して、投票選択手段にデコミットメッセージを送る場合を除く。投票生成センターまたは投票選択手段または投票集計センターは、ミキシングセンターまたは投票集計センターとしても機能する。パーソナルコンピュータは、上述の方式を実施するソフトウェアを内蔵するか、または、図２に示した要素をハードウェアやソフトウェア内に有している。

【００６１】図２は、レシートフリー投票を実現するためにメッセージがどのように転送されるかを示す。上述したように、投票生成センター１０は、各投票選択手段１２（ｉ）に対して、投票構成プロセス２６を用いて暗号化投票を生成する。投票生成センターはつぎに、コミットメントアルゴリズム２１、「１－０」証明アルゴリズム２２、デコミットメントアルゴリズム２３からなる証明プロセス２０を実行する。デコミットメントの出力は、盗聴不可能なチャンネル１６（ｉ）を介して投票選択手段１２（ｉ）に送られる。投票生成センター１０のその他の出力は電子掲示板１３上に送付される。投票選択手段１２（ｉ）は、検証プロセス２４および選択プロセス２５を実行し、掲示板上の暗号化投票から選択した投票を出力する。すべての投票選択手段１２（１）、１２（２）、…、１２（ｌ）の選択した投票は、匿名チャンネル１４を介して投票集計センター１５に無記名で転送される。

【００６２】図３は、シャッフルネットを用いた本発明の好ましい実施形態を概略的に示している。投票生成センター１０と、投票シャッフリングセンター１１（１）、１１（２）、…、１１（ｍ）と、投票選択手段１２（１）、１２（２）、…、１２（ｌ）と、ミキシングセンター１４（１）、１４（２）、…、１４（ｎ）と、投票集計センター１５は、従来の電子掲示板１３に接続されたパーソナルコンピューターまたはワークステーションを用いている。盗聴不可能なチャンネル１６（１）、１６（２）、…、１６（ｌ）を設けて、投票生成センターから各投票選択手段に秘密メッセージを送ることができるように構成されている。さらに、盗聴不可能なチャンネル１７（１）、１７（２）、…、１７．（ｍ）を設けて、シャッフリングセンター１１（１）、

15

11（2）、…、11（m）から投票選択手段12（i）に秘密メッセージを送ることができる構成されている。メッセージ転送プロセスを構成するすべての要素（送出部、検証手段、センターなど）は、掲示板にメッセージを送付したりそこからメッセージを受け取ったりすることにより相互に働きかける。ただし、投票生成センターやシャッフリングセンターが、盗聴不可能なチャンネルを介して投票選択手段にデコミットメッセージを送る場合を除く。投票生成センターまたは投票選択手段または投票集計センターまたはシャッフリングセンターは、ミキシングセンターまたは投票集計センターまたはシャッフリングセンターとしても機能する。パーソナルコンピュータは、上述の方式を実施するソフトウェアを内蔵するか、または、図4および図5に示した要素をハードウェアやソフトウェア内に有している。

【0063】図4は、シャッフルネットを用いてレシートフリー投票を実現するためにメッセージがどのように転送されるかを示す。投票生成センター10は、各投票選択手段12（i）に対して暗号化投票を生成し、電子掲示板13上に送付する。つぎにシャッフリングセンター11（1）は、掲示板13から暗号化投票を読み、シャッフルプロセス30および証明プロセス31を実行し、シャッフルした投票を掲示板13に出力する。その一方で、盗聴不可能なチャンネル17（1）を介して投票選択手段12（i）にデコミットメッセージを送る。同様にして、以降のシャッフリングセンターは掲示板13から前のセンターの出力を読み、自己の出力をつぎのシャッフリングセンターに与えるために掲示板に送付する。その一方で、盗聴不可能なチャンネル17（1）を介して投票選択手段12（i）にデコミットメッセージを送る。投票選択手段12（i）は最後のシャッフリングセンターの出力を読み、検証プロセス35と選択プロセス36を実行し、掲示板上の暗号化投票から選択した投票を出力する。すべての投票選択手段12（1）、12（2）、…、12（l）の選択した投票は、匿名チャンネル14を介して投票集計センター15に無記名で転送される。

【0064】投票生成センターがそのランダムストリングをデコミットした後、投票選択手段12（i）は、無効化プロセス37を行ない、センターのコミットメントを無効化する。

【0065】図5は、シャッリングセンター11（i）を概略的に示す図である。シャッフリングセンターはシャッフルプロセス30と証明プロセス31を行なう。証

16

明プロセス31は、コミットメントアルゴリズム32、証明シャッフルアルゴリズム33、デコミットメントアルゴリズム34を含む。

【0066】以上、安全なレシートフリー電子投票のための好ましい方式および装置について説明したが、当業者であれば、請求項により定められる本発明の開示および趣旨の範囲を逸脱することなく変形や修正が可能であることはいうまでもない。

【図面の簡単な説明】

【図1】本発明の好ましい一実施形態の概略図である。

【図2】メッセージの流れの概略図である。

【図3】シャッフリングセンターを設けた本発明の好ましい実施形態の概略図である。

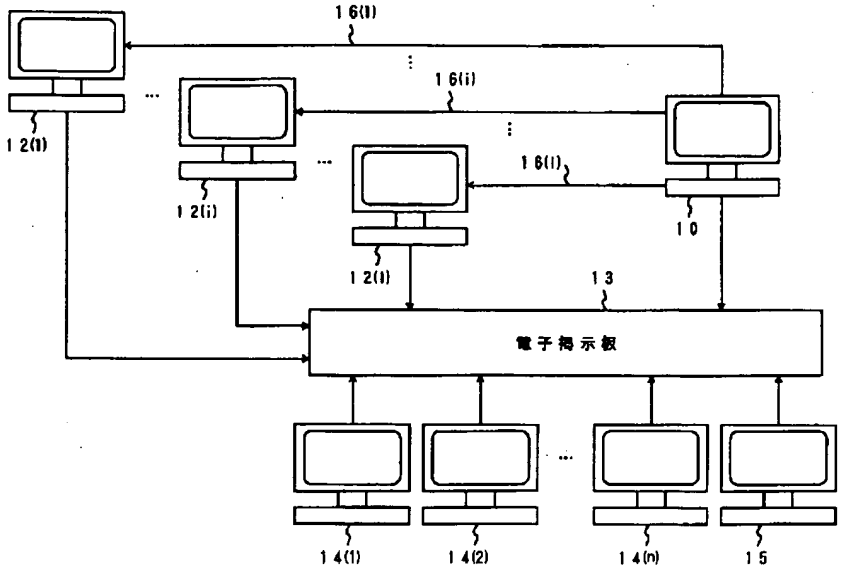
【図4】シャッフリングセンターを設けた場合のメッセージの流れの概略図である。

【図5】シャッフリングセンターの概略図である。

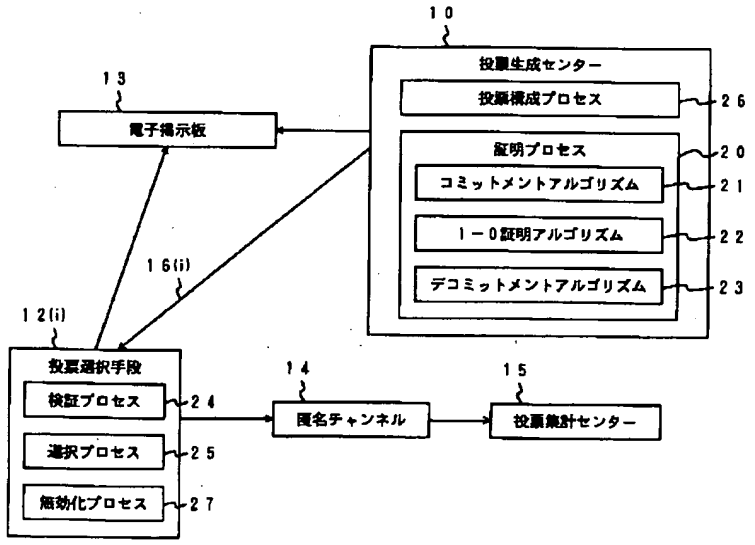
【符号の説明】

10	投票生成センター
11	シャッフルネット
11（i）	シャッフリングセンター
12（i）	投票選択手段
13	電子掲示板
14	匿名チャンネル
14（1）～n	ミキシングセンター
15	投票集計センター
16（i）	盗聴不可能なチャンネル
17（1）～m	盗聴不可能なチャンネル
20	証明プロセス
21	コミットメントアルゴリズム
22	1－0証明アルゴリズム
23	デコミットメントアルゴリズム
24	検証プロセス
25	選択プロセス
26	投票構成プロセス
27	無効化プロセス
30	シャッフルプロセス
31	証明プロセス
32	コミットメントアルゴリズム
33	証明シャッフルアルゴリズム
34	デコミットメントアルゴリズム
35	検証プロセス
36	選択プロセス
37	無効化プロセス

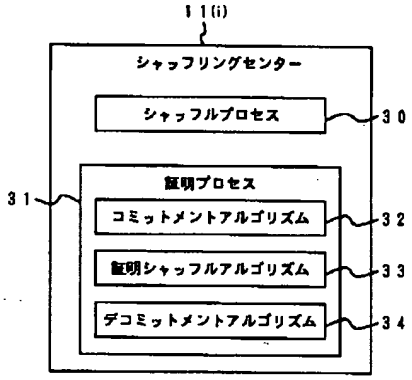
【図1】


16(1)
16(i)
16(l)
12(1)
12(i)
12(l)
10
13
電子掲示板
14(1)
14(2)
14(n)
15

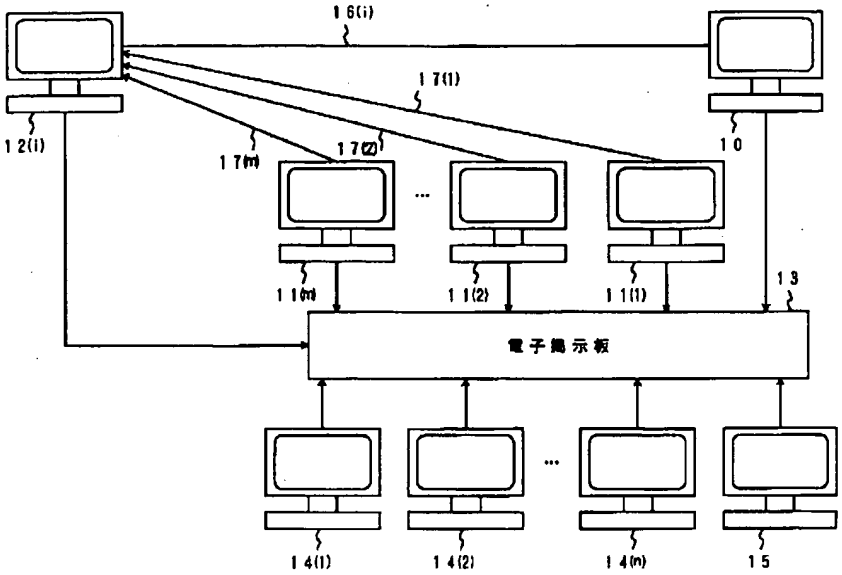
【図2】


10
投票生成センター
投票構成プロセス
26
証明プロセス
20
コミットメントアルゴリズム
21
1－0証明アルゴリズム
22
デコミットメントアルゴリズム
23
13
電子掲示板
16(i)
12(i)
投票選択手段
検証プロセス
24
選択プロセス
25
無効化プロセス
27
14
匿名チャンネル
15
投票集計センター

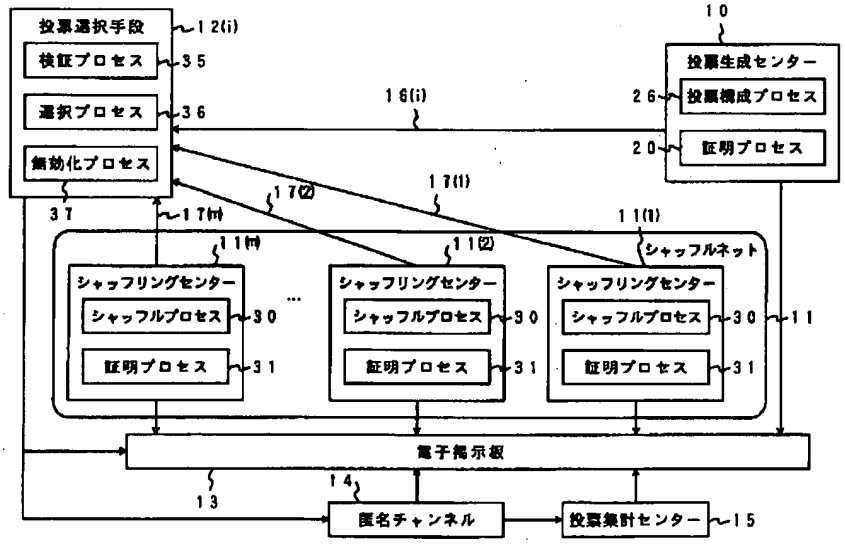
【図5】


11(i)
シャッフリングセンター
シャッフルプロセス
30
証明プロセス
31
コミットメントアルゴリズム
32
証明シャッフルアルゴリズム
33
デコミットメントアルゴリズム
34

【図3】


16(i)
17(1)
12(i)
17(m)
17(2)
10
11(m)
11(2)
11(1)
13
電子掲示板
14(1)
14(2)
14(n)
15

【図4】


投票選択手段
12(i)
検証プロセス
35
選択プロセス
36
無効化プロセス
37
10
投票生成センター
26
投票構成プロセス
16(i)
20
証明プロセス
17(2)
17(1)
17(m)
11(1)
11(m)
11(2)
シャッフルネット
シャッフリングセンター
シャッフルプロセス
30
証明プロセス
31
11
電子掲示板
13
14
匿名チャンネル
投票集計センター
15

【外国語明細書】

1. Title of Invention

Secure Receipt-Free Electronic Voting

2. Claims

1. A method of secure receipt-free voting comprising the steps of:

   (a) constructing votes for each vote chooser which votes are posted on a bulletin board;

   (b) sending private messages to respective vote choosers without being intercepted;

   (c) the vote chooser choosing the vote and constructing a message;

   (d) the message from the vote chooser reaching a vote counting center through a secure anonymous channel; and

   (e) the vote counting center counting the votes.

2. A method of secure receipt-free voting as set forth in claim 1, where said sending private messages comprises sending via secure untappable channels.

3. A method of secure receipt-free voting as set forth in claim 1, further comprising the step of proving the correctness of the vote construction.

4. A method of secure receipt-free voting as set forth in claim 3, where proving the correctness is performed by executing algorithm prove 1-0.

5. A method of secure receipt-free voting as set forth in claim 3, further comprising the steps of:

   (f) said constructing votes including committing a random string using chameleon commitments;

   (g) proving the correctness of the constructed votes by using committed bits; and

(h) decommiting through a secure untappable channel.

6. A method of secure receipt-free voting as set forth in claim 5, where proving the correctness is performed by executing the algorithm prove 1-0.

7. A method of secure receipt-free voting as set forth in claim 5, further comprising the vote chooser invalidating chameleon commitment.

8. A method of secure receipt-free voting as set forth in claim 7, where proving the correctness is performed by executing the algorithm prove 1-0.

9. A method of secure receipt-free voting as set forth in claim 7, where the vote chooser invalidating chameleon commitment provides its secret key for constructing votes to the bulletin board.

10. A method of secure receipt-free voting as set forth in claim 1, where step (a) further comprises:

(i) shuffling the constructed votes; and

(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

11. A method of secure receipt-free voting as set forth in claim 10, where said sending a private message comprises sending via a secure untappable channel.

12. A method of secure receipt-free voting as set forth in claim 2, where step (a) further comprises:

(i) shuffling the constructed votes; and

(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

13. A method of secure receipt-free voting as set forth in claim 4, where said sending a private message comprises sending via a secure untappable channel.

14. A method of secure receipt-free voting as set forth in claim 5, where step (a) further comprises:

    (i) shuffling the constructed votes; and

    (ii) sending a private message about the shuffling to the vote chooser without being intercepted.

15. A method of secure receipt-free voting as set forth in claim 14, where said sending a private message comprises sending via a secure untappable channel.

16. A method of secure receipt-free voting as set forth in claim 7, where step (a) further comprises:

    (i) shuffling the constructed votes; and

    (ii) sending a private message about the shuffling to the vote chooser without being intercepted.

17. A method of secure receipt-free voting as set forth in claim 16, where said sending a private message comprises sending via a secure untappable channel.

18. A method of secure receipt-free voting as set forth in claim 3, where step (a) further comprises:

    (i) shuffling the constructed votes; and

    (ii) sending a private message about the shuffling to the vote chooser without being intercepted.

19. A method of secure receipt-free voting as set forth in claim 18, where said sending a private message comprises sending via a secure untappable channel.

20. A method of secure receipt-free voting as set forth in claim 10, further comprising the step of proving the correctness of the shuffled constructed votes.

21. A method of secure receipt-free voting as set forth in claim 20, further comprising the steps of:

(f) committing a random string using chameleon commitments;

(g) proving the correctness of the shuffled constructed votes using committed bits; and

(h) decommiting without being intercepted.

22. A method of secure receipt-free voting as set forth in claim 21 where said decommiting is through a secure untappable channel.

23. A method of secure receipt-free voting as set forth in claim 20, where said proving the correctness is performed by executing the algorithm prove shuffle.

24. A method of secure receipt-free voting as set forth in claim 21, where said proving the correctness is performed by executing the algorithm prove shuffle.

25. A method of secure receipt-free voting as set forth in claim 21, further comprising invalidating the chameleon commitment.

26. A method of secure receipt-free voting as set forth in claim 23, further comprising invalidating the chameleon commitment.

27. A method of secure receipt-free voting as set forth in claim 26, where the said invalidating chameleon commitment includes providing a secret key for said shuffling to the bulletin board.

28. An apparatus for secure receipt-free voting comprising:

a plurality of vote generating centers;

a plurality of vote choosers;

a bulletin board;

a vote counting center;

said vote generating centers constructing votes for each said vote chooser which votes are posted on said bulletin board and said vote generating centers sending private messages to respective vote choosers without being intercepted;

each said vote chooser choosing the vote and constructing a message which reaches said vote counting center through a secure anonymous channel; and

said vote counting center counting the votes.

29. An apparatus for secure receipt-free voting as set forth in claim 28, where said vote generating centers send private messages to said vote choosers via secure untappable channels.

30. An apparatus for secure receipt-free voting as set forth in claim 28, further comprising:

said vote generating center committing a random string using chameleon commitment; proving the correctness of the vote construction using committed bits; and decommiting through a secure untappable channel.

31. An apparatus for secure receipt-free voting as set forth in claim 30, further comprising said vote chooser invalidating the chameleon commitment.

32. An apparatus for secure receipt-free voting as set forth in claim 28, further comprising:

a shuffle net of shuffling centers for receiving said constructed votes; and

each shuffling center in the shuffle net shuffling the votes and sending a private message to a vote chooser without being intercepted.

33. An apparatus for secure receipt-free voting as set forth in claim 32, where each shuffling center sends a private message to a vote chooser via a secure untappable channel.

34. An apparatus for secure receipt-free voting as set forth in claim 30, further comprising:

a shuffle net of shuffling centers for receiving said constructed votes; and

each shuffling center in the shuffle net shuffling the votes and sending a private message to a vote chooser without being intercepted.

35. An apparatus for secure receipt-free voting as set forth in claim 34, where each shuffling center sends a private message to a vote chooser via a secure untappable channel.

36. An apparatus for secure receipt-free voting as set forth in claim 32, further comprising said shuffling centers proving the correctness of their vote construction.

37. An apparatus for secure receipt-free voting as set forth in claim 36, further comprising:

each shuffling center committing a random string using chameleon commitment and proving the correctness of its vote using committed bits, and decommiting without being intercepted.

38. An apparatus for secure receipt-free voting as set forth in claim 37 where said decommiting is through a secure untappable channel.

39. An apparatus for secure receipt-free voting as set forth in claim 37, further comprising each vote chooser invalidating the chameleon commitment.

40. An apparatus for secure receipt-free voting as set forth in claim 39, where each vote chooser invalidating the chameleon commitment by providing its secret key to said shuffling centers or to said bulletin board.

3. Detailed Description of Invention

Field of Invention

The present invention relates to a method and apparatus useful for secure receipt-free electronic voting and specifically, to number-theoretic based algorithms for secure receipt-free electronic voting.

Background of the Invention

The ultimate goal of secure electronic voting is to replace physical voting booths. Achieving this goal requires work both on improving the efficiency of current protocols and understanding the security properties that these physical devices can provide.

Recently, it is observed in an article by J.C. Benaloh et al, entitled "Receipt-free Secret-ballot Election," in STOC 94, pp. 544-553 (1994), that unlike physical voting protocols, nearly all electronic voting protocols give the voters a receipt by which they can prove how they voted. Such receipts provide a ready means by which voters can sell their votes or by which another party can coerce a voter to vote in a certain way.

Benaloh and Tuinstra give the first receipt-free protocol for electronic voting. In their scheme a trusted center generates for each voter a pair of ballots consisting of a "yes" vote and a "no" vote in random order. Using a trusted beacon and a physical voting booth the center proves to the public that the ballot indeed includes a well-formed (yes/no) or (no/yes) pair and at the same time proves to the verifier which pair it is. The physical apparatus ensures that by the time the

verifier is able to communicate with an outsider, the verifier can forge a proof that the ballot is (yes/no) and also forge a proof that it is (no/yes). Thus, such a proof ceases to provide either proof as a receipt.

Independently, Niemi and Renvall tried to solve this problem in an article by Niemi et al, entitled "How to prevent buying of votes in computer elections" in ASIACRYPT '94, pp. 141-148 (1994). They also use a physical voting booth where a voter performs multiparty computation with all the centers.

Both the Benaloh-Tuinstra and the Niemi-Renvall protocols illustrate that receipt-free secure voting is possible. However, their physical requirements are fairly cumbersome, and are not unlike those faced by participants in physical elections. An important open question is precisely what physical requirements are necessary for achieving receipt-free secure voting.

In accordance with the teachings of the present invention, a secure receipt-free voting scheme is described with a more practical physical requirement, that is the existence of a physically secure untappable private channel.

Summary of the Invention

A secure receipt-free voting scheme is described where each voter does not leave evidence of how the voter voted by using a physically secure untappable channel. The term "untappable secure channel" refers to the fact that a message can be sent from a center without being accessed or detected by another party. Such an untappable channel is described in an article by C. Bennett et al entitled "Quantum Cryptography" in Scientific American, vol. 267, no. 4, Oct. 1992, pp. 50 to 57. The end result of using an untappable channel is that neither the voter nor another party can show or prove how a vote was cast or what was the message that was sent. Once a message is sent or received, the content may be changed rendering proof of the message impossible. However, if the message is intercepted or detected in route or at the time of reception, the intercepting or detecting party can learn the content of a message prior to a time when a change was possible. Moreover, even if a non-secure channel is used, if the message travels along the channel without interruption or detection, by virtue of the protocol used in the present invention, determination of a particular vote after receipt at its destination is not possible. In other words, an untappable channel refers to the transmission

of a message without interception or detection in route.

In the following description, the term 'chameleon commitments' is used. A chameleon commitment is a message committing and decommiting protocol, where the committer can decommit as the committer committed, while the receiver can decommit in any way, regardless of how the committer committed.

In accordance with the method of the present invention, there is a vote generating center, a vote counting center, and shuffling centers to transfer messages between the various centers and each voter. The method comprises the following three steps.

The first step is the generation by a voter generating center of a set of all possible votes for each voter. For simplicity, it will be assumed that the possible votes are two, namely 1-vote and 0-vote. For each voter i, the vote generating center posts encrypted 1-votes and 0-votes in random order. The committer commits to the ordering using chameleon bit commitments. The center proves that the committer constructed the vote-pairs properly. The committer decommits the ordering only to the voter through an untappable secure channel.

The second step is the transferring the vote from the vote generating center to the voter via the shuffling centers. Each shuffling center shuffles the two votes for voter i through a shuffle-net. The committer commits with regard to how the votes are shuffled using chameleon commitments. Each shuffling center proves the correctness of its action. The committer reveals how the votes were shuffled only to the voter i through an untappable secure channel.

The second step is not mandatory, in which case the vote generating center may directly send the vote to the voter through an ordinary channel.

The third step is anonymous voting by the voter. By keeping track of the initial ordering of the pair, and how they were shuffled during the second step, each voter knows which vote is which. Each voter submits one of the received votes to the counting center through a secure anonymous channel. Then the counting center tallies the votes.

Implementation of a secure anonymous channel can be found in an article by

C. Park et al entitled "Efficient Anonymous Channel and All/Nothing Election Scheme" in Advances in Cryptology, Eurocrypt '93, 1993, pp. 248 to 259, or in pending U.S. patent application serial number 08/376,568 entitled "Secure Anonymous Message Transfer and Voting Scheme" which is assigned to the same assignees as the present invention. Also, the invention results in a method which reduces the amount of communication and computation necessary to generate, transmit and check the proofs by combining multiple proofs into a single proof.

The present invention will be best understood when the following description is read in conjunction with the accompanying drawing.

Detailed Description of the Invention

A preferred embodiment of a secure receipt-free voting scheme comprising the present invention will now be described with reference to Figures 1 and 2. In accordance with the scheme, the encrypted votes generated by vote generating center 10 by vote construct process 26 are posted on an electronic bulletin board 13 or other publicly accessible messaging means. The encrypted votes are pairs of 1-votes and 0-votes, permuted in random order, for each vote chooser 12(i). Then the vote generating center 10 secretly conveys to the vote chooser 12(i)

through an untappable channel 16(i) how the encrypted votes for vote chooser 12(i) is ordered. At the same time, the vote generating center 10 needs to prove to the public that the vote was honestly generated and to the vote chooser that the center 10 had not sent false information in the secret message. These proofs are achieved by following prove process 20 as will be described below.

The vote chooser 12(i) chooses its ballot using the secret message from the vote generating center 10 through a physically untappable channel 16(i). The vote chosen by the vote choosers 12(1), 12(2), ...12(ℓ) are transferred anonymously through a secure anonymous channel to a vote counting center 15. The secure anonymous channel can be realized by the mixing centers 14(1), 14(2), ...14(n), where encrypted votes are successively processed by the mixing centers until the vote counting center 15 provides as its output a randomly, untraceably ordered set of unencrypted votes and the outcome of the tally. Each vote generating center 10, vote chooser 12(i), mixing center 14(i) and vote counting center 15 comprises a computing means, preferably a personal computer but it may also be a work-station or the like.

Having set forth an overview of the scheme, the detail of vote construct process 26, prove process 20, and the information being transferred securely through untappable channel 16 will now be described.

The vote generating center 10, by executing vote construct process 26, generates an encrypted pair of 0-vote and 1-vote for each vote chooser 12(i). The center follows the vote construct process for each vote chooser 12(i) with independently chosen random numbers.

The encrypted form of 1-votes and 0-votes need to be appropriate for input to the anonymous channel. Preferably, the method and apparatus described in U.S. patent application 08/376,568 which is incorporated herein by reference, is used and the encrypted forms of 1-votes and 0-votes are selected to be:

$$v_i^0 = (g^{r_{i1}} \bmod p,\ m_0 \cdot y^{r_{i1}} \bmod p)$$
$$v_i^1 = (g^{r_{i2}} \bmod p,\ m_1 \cdot y^{r_{i2}} \bmod p) \qquad (1)$$

for independent random numbers r_{i1} and r_{i2} for vote chooser 12(i) and appropriately chosen common constants p, g, y, m_0 and m_1 for all vote choosers. The vote construct process 26 comprises calculating the above formulas with randomly

chosen numbers r_{i1} and r_{i2}.

The vote generating center 10 posts on the bulletin board in the order of (v_i^0, v_i^1) with probability of one half and (v_i^1, v_i^0) otherwise.

The prove process 20 comprises three algorithms: commitment 21, prove 1-0 22, and decommitment 23. The algorithm commitment 21 is used to calculate and post a chameleon commitment of the above ordering and a random sequence used in the succeeding prove 1-0 protocol. The algorithm prove 1-0 is executed multiple times to prove that the center 10 generated the votes honestly, and the output is posted on bulletin board 13. The algorithm decommit 23 is used to decommit the chameleon commitment committed in algorithm commit 21, through an untappable secure channel. The specific algorithms of prove 1-0 and chameleon commitment/decommitment will be described below.

The vote generating center sends an output of a decommitter, which is a chameleon decommitment, to the vote chooser i through the untappable channel.

The vote chooser 12(i) verifies the correctness of the prove 1-0 algorithm and the validity of decommitments by verification process 24. If the correctness and validity are verified, the vote chooser 12(i) follows selection process 25 and chooses either one of the encrypted votes on the bulletin board, which expresses its opinion. The vote chooser is able to choose correctly because it would know how the encrypted votes were ordered from the chameleon decommitment.

The vote chosen by the vote chooser 12(i) will be input to a shuffle-net, together with other votes chosen by the other vote choosers.

Applying the scheme described above, a malicious party who coerces the vote chooser 12(i) to disclose its vote, will not receive a concrete proof of whether the chosen vote was a 1-vote or a 0-vote unless the vote generating center 10 is allowed to disclose the vote or the secure channel 16(i) is tapped into.

The algorithms prove 1-0 and chameleon commitment/decommitment will now be described. The prove 1-0 algorithm involves a prover and a verifier. The prover is the vote generating center in this case. The verifier may be any entity, including vote choosers. The probabilistic behavior of the algorithm will be de-

termined by an output of a suitable hash function, but it may also be a random beacon.

The algorithm comprises, given randomly permuted pair of (v_i^0, v_i^1) generated and posted as equations (1), showing that they are indeed a pair of 1-vote and 0-vote. Assume a random string has been committed using chameleon commitment to the vote chooser.

prove 1-0

1 The prover uniformly chooses r', r'' and calculates

$$E_0(v^0) = (g^{r'} \bmod p,\ m_0 \cdot y^{r'} \bmod p)$$
$$E_1(v^1) = (g^{r''} \bmod p,\ m_1 \cdot y^{r''} \bmod p)$$

and posts $E_0(v^0), E_1(v^1)$ in the order according to the committed string.

2a. With probability $\frac{1}{2}$, the prover is asked to reveal r' and r''. The verifier checks if $E_0(v^0), E_1(v^1)$ is made consistently.

2b. With probability $\frac{1}{2}$, the prover is asked to reveal $s1 = r_{i1} - r'$ and $s2 = r_{i2} - r''$. The verifier checks that v_i^0 and v_i^1 can be indeed generated from $E_0(v^0), E_1(v^1)$ using $s1, s2, g$ and y.

The chameleon commitment scheme will now be described. The chameleon commitment scheme involves a sender and a receiver. The sender is the vote generating center in this case. The receiver are the vote choosers.

The following is explained in terms of committing a single bit, 0 or 1, but can be easily transformed to commit multiple bits and strings. In the scheme, the receiver is assumed to know a satisfying $\alpha = g^a$ for public integer α.

Commitment Sender commits 0 by g^r and $\alpha \cdot g^r$ for 1 to the receiver.

Decommitment Sender reveals r. The receiver calculates both g^r and $\alpha \cdot g^r$ and determines what was the committed bit.

In order to modify the decommitment, the receiver may claim it received $r - a$ instead of r, which is the case when the sender committed the other value.

A more detailed description of chameleon commitments can be found in article "Minimum Disclosure Proofs of Knowledge" by Brassard, Chaum and Crépeau in *JCSS*, pages 156–189, 1988.

After the vote generating center decommitted its random string, the vote chooser 12(i) may follow with invalidation process 27 to invalidate the commitment of the center. The invalidation process 27 comprises informing the center of the value a, so that the center also has the ability to provide false information afterwards, or to post the value a on a bulletin board 13.

To make sure that the vote chooser has the ability to modify the commitments, that is, the vote chooser knows the exponent a, the interaction may occur between the vote generating center and each vote chooser, before the commitment is applied, or even before the start of voting. For example, the vote choosers may execute a cut-and-choose protocol to pick the constant α so that the vote chooser knows a with high probability.

In order to make the receipt-free property more secure, it is possible to incorporate a shuffle net 11 comprising multiple shuffling centers 11(1), 11(2),...11(m), as shown in Figures 3 and 4. Each encrypted vote generated by vote generating center 10 for vote chooser 12(i) is passed through shuffle net 11 before reaching the vote chooser 12(i). As a result of so doing, a malicious party would not be able to determine how the vote chooser 12(i) voted unless it colluded with all the shuffling centers and vote generating centers, or wiretapped every secret channel 17(1), 17(2), ...17(m) between the shuffling centers and the vote chooser 12(i).

Each vote shuffling center comprises a computing means, preferably a personal computer but it may also be a workstation or the like.

The operation of the shuffle net and shuffling centers will now be described. Shuffling center 11(j) processes each message posted by the previous shuffling center 11($j-1$) (or the vote generating center 10, when $j = 1$) and posts the results of process shuffle 30 (Figure 5) in permuted order until the last shuffling center 11(m) posts the result of the shuffling. Each shuffling center conveys how the votes were

shuffled to the vote chooser through an untappable secure channel 17(j). Each shuffling center proves it shuffled honestly and did not provide false information to the vote chooser in a manner similar to that of the vote generating center, which is achieved through executing process prove 31.

Figure 5 illustrates the operation of a shuffling center 11(i). The shuffling center 11(i) executes the processes shuffle 30 and prove 31 and posts the outputs. The process prove 31 comprises an algorithm commitment 32 which chameleon commits the random string to the vote chooser.

The process prove 31 further comprises three algorithms: commitment 32, prove shuffle 33, and decommitment 34.

In order to describe the process shuffle 30, let the input be encrypted shuffled votes, which are presented as:

$$X_1 = (A_1, A_2)$$
$$X_2 = (B_1, B_2)$$

The algorithm shuffle comprises generating a random number c_1 and c_2 and shuffling the encrypted votes X_1 and X_2 as

$$S(X_1) = (A_1 \cdot g^{c_1} \bmod p,\ A_2 \cdot y^{c_1} \bmod p)$$
$$S(X_2) = (B_1 \cdot g^{c_2} \bmod p,\ B_2 \cdot y^{c_2} \bmod p) \qquad (2)$$

and posting $S(X_1)$ and $S(X_2)$ in random order.

This order and a random sequence to be used in the algorithm prove shuffle is committed using chameleon commitment and posted on the bulletin board as the output of algorithm commitment 32.

The algorithm prove shuffle 33 is used to prove that the shuffling center executed the algorithm shuffle correctly. The prove-shuffle algorithm involves a prover and a verifier. The prover is the shuffling center in this case. The verifier may be any entity, including a vote chooser. The probabilistic behavior of the algorithm will be determined by an output of a suitable hash function, but it may also be a random beacon. The algorithm comprises a permuted pair of $(S(X_1), S(X_2))$,

showing that they are indeed generated from inputs X_1 and X_2 as equations (2). Assume a random string has been committed using chameleon commitment to the vote chooser.

prove shuffle

1. The prover uniformly chooses c', c'' and calculates

$$E(X_1) = (A_1 \cdot g^{c'} \bmod p,\ A_2 \cdot y^{c'} \bmod p)$$
$$E(X_2) = (B_1 \cdot g^{c''} \bmod p,\ B_2 \cdot y^{c''} \bmod p)$$

post $E(X_1), E(X_2)$ in the order according to the committed string.

2a. With probability $\frac{1}{2}$, the prover is asked to reveal c' and c''. The verifier checks if $E(X_1), E(X_2)$ is made consistently.

2b. With probability $\frac{1}{2}$, the prover is asked to reveal $t_1 = c_1 - c'$ and $t_2 = c_2 - c''$. The verifier checks that $E(X_1)$ and $E(X_2)$ can indeed be generated from $S(X_1), S(X_2)$ using t_1, t_2, g and y.

The encrypted votes posted by the vote generating centers are successively processed by the shuffling centers 11(1), 11(2), ...11(m) until the last center provides as its output a randomly, untraceably ordered set of encrypted votes for each vote chooser.

The vote chooser 12(i) chooses its ballot using the secret messages from the vote generating center and shuffling centers through untappable secure channels 16(i), 17(1),17(2), ... and 17(m).

Invalidation of chameleon commitments of shuffling centers can be realized in a similar manner as invalidated commitments of vote generating center.

Having described a preferred method of practicing the present invention, preferred embodiments useful for practicing the invention will now be described.

Figure 1 schematically illustrates a preferred embodiment for practicing the invention. The vote generating center 10, vote choosers 12(1), 12(2), ...12(ℓ), mixing

centers 14(1), 14(2), ...11(n) and vote counting center 15 use personal computers or workstations connected to a conventional electronic bulletin board 13. There are untappable secure channels 16(1),16(2) ... 16(ℓ) so that the vote generating center can send a secret message to each vote chooser. All elements (senders, verifiers, centers and the like) comprising the message transfer process interact by posting messages to and receiving messages from the bulletin board 13, except when the vote generating center sends decommitting messages to vote choosers via untappable channel 16. The vote generating center or vote choosers or vote counting center can also serve as mixing centers or vote counting centers. The personal computers either contain software to perform the method described above or alternatively contain in hardware or software embodiments of the elements described in Figure 2.

Figure 2 illustrates how messages are transferred to achieve receipt-free voting. For each vote chooser 12(i), vote generating center 10 generates encrypted votes using a vote constructor 26 as described above. The vote generating center then follows process prove 20 which comprises algorithms commitment 21, prove 1-0 22 and decommitment 23. The output of decommitment is sent to vote chooser 12(i) through untappable channel 16(i). Other outputs of the vote generating center 10 is posted on the bulletin board 13. The vote chooser 12(i) follows the processes verification 24 and selection 25, and outputs selected votes from the encrypted votes on the bulletin board. The selected votes of all the vote choosers 12(1), 12(2) ...12(ℓ) are anonymously transferred to vote counter 15 through anonymous channel 14.

Figure 3 schematically illustrates a preferred embodiment for practicing the invention with a shuffle net. The vote generating center 10, vote shuffling centers 11(1), 11(2), ...11(m), vote choosers 12(1), 12(2), ... 12(ℓ), mixing centers 14(1), 14(2), ...11(n) and vote counting center 15 use personal computers or workstations connected to a conventional electronic bulletin board 13. There are untappable channels 16(1),16(2) ... 16(ℓ) so that the vote generating center can send a secret message to each vote chooser. There are also untappable channels 17(1),17(2) ...17(m) so that the shuffling centers 11(1), 11(2), ...11(m) can send a secret message to vote chooser 12(i). All elements (senders, verifiers, centers and the like) comprising the message transfer process interact by posting messages to and receiving messages from the bulletin board, except for the vote generating center or shuffling centers which send decommitting messages to a vote chooser via un-

tappable channels. The vote generating center or vote choosers or vote counting center or shuffling centers can also serve as mixing centers or vote counting centers or shuffling centers. The personal computers either contain software to perform the method described above or alternatively contain in hardware or software embodiments the elements described in Figures 4 and 5.

Figure 4 illustrates how messages are transferred to achieve receipt-free voting with a shuffle net. For each vote chooser 12(i), vote generating center 10 generates encrypted votes which are posted on the bulletin board 13. Then shuffling center 11(1) reads encrypted votes from the bulletin board 13 and follows processes shuffle 30 and prove 31, and output shuffled votes to the bulletin board 13, while sending a decommitting message to vote chooser 12(i) through untappable channel 17(1). Similarly, the succeeding shuffling centers read the proceeding centers output from bulletin board 13, and post its output to the bulletin board for the next shuffling center, while sending its decommitting message to vote chooser 12(i) through untappable channel 17(1). The last shuffling center's output will be read by the vote chooser 12(i), which follows the processes verification 35 and selection 36, and outputs selected votes from the encrypted votes on the bulletin board. The selected votes of all the vote choosers 12(1), 12(2) ... 12(ℓ) are anonymously transferred to vote counter 15 through anonymous channel 14.

Figure 5 schematically illustrates a shuffling center 11(i). The shuffling center follows process shuffle 30 and process prove 31. Process prove 31 comprises algorithms commitment 32, prove shuffle 33 and decommitment 34.

While there has been described and illustrated a preferred method and apparatus of secure receipt free electronic voting, it will be apparent to those skilled in the art that variations and modifications are possible without deviating from the broad teachings and spirit of the present invention which shall be limited solely by the scope of the claims appended hereto.

4. Brief Description of Drawings

Figure 1 is a schematic illustration of a preferred embodiment for practicing the present invention;

Figure 2 is a schematic illustration of message flow;

Figure 3 is a schematic illustration of a preferred embodiment for practicing the present invention with shuffling centers;

Figure 4 is a schematic illustration of a message flow with shuffling centers; and

Figure 5 is a schematic illustration of a shuffling center.

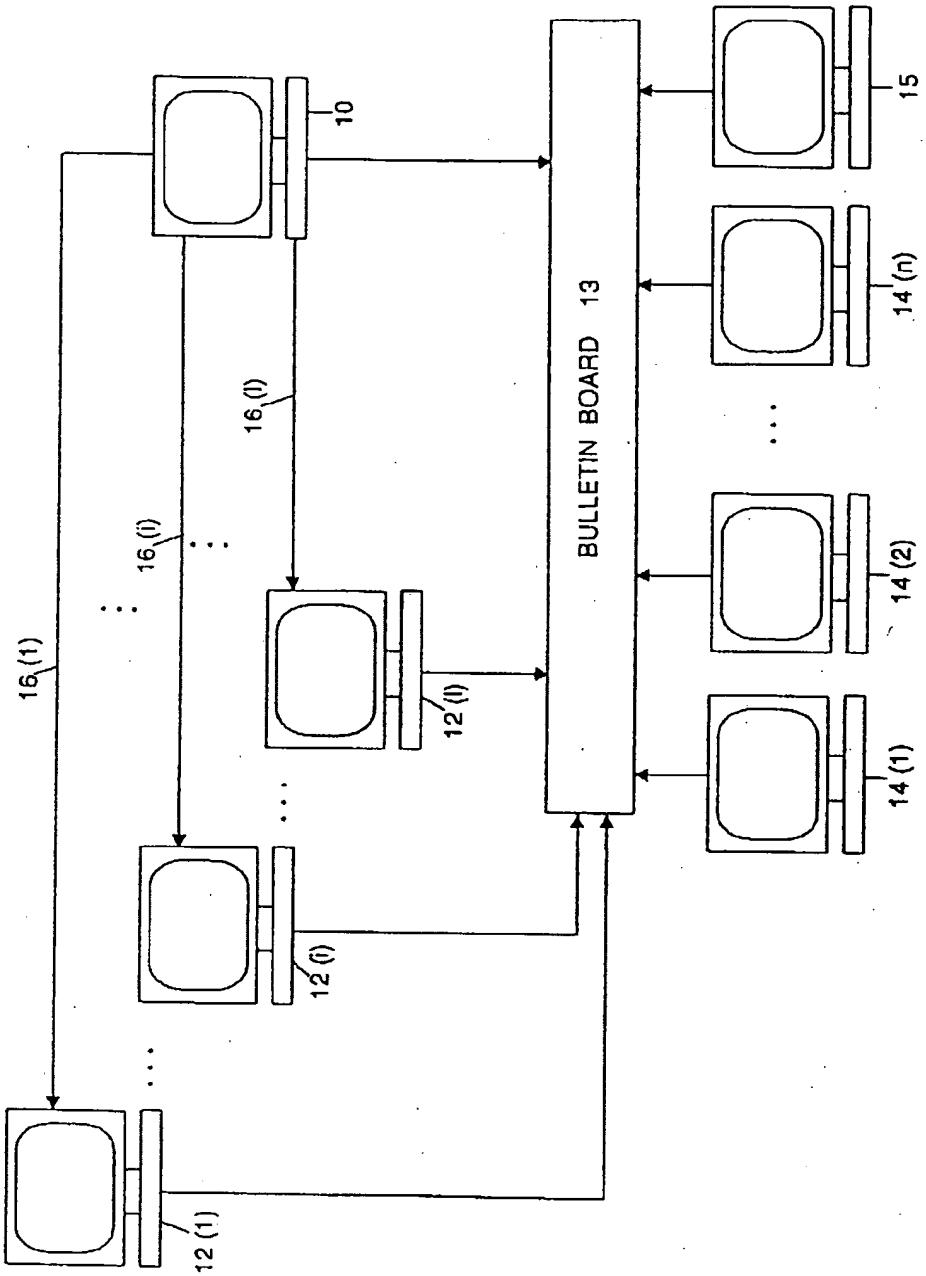


FIG 1

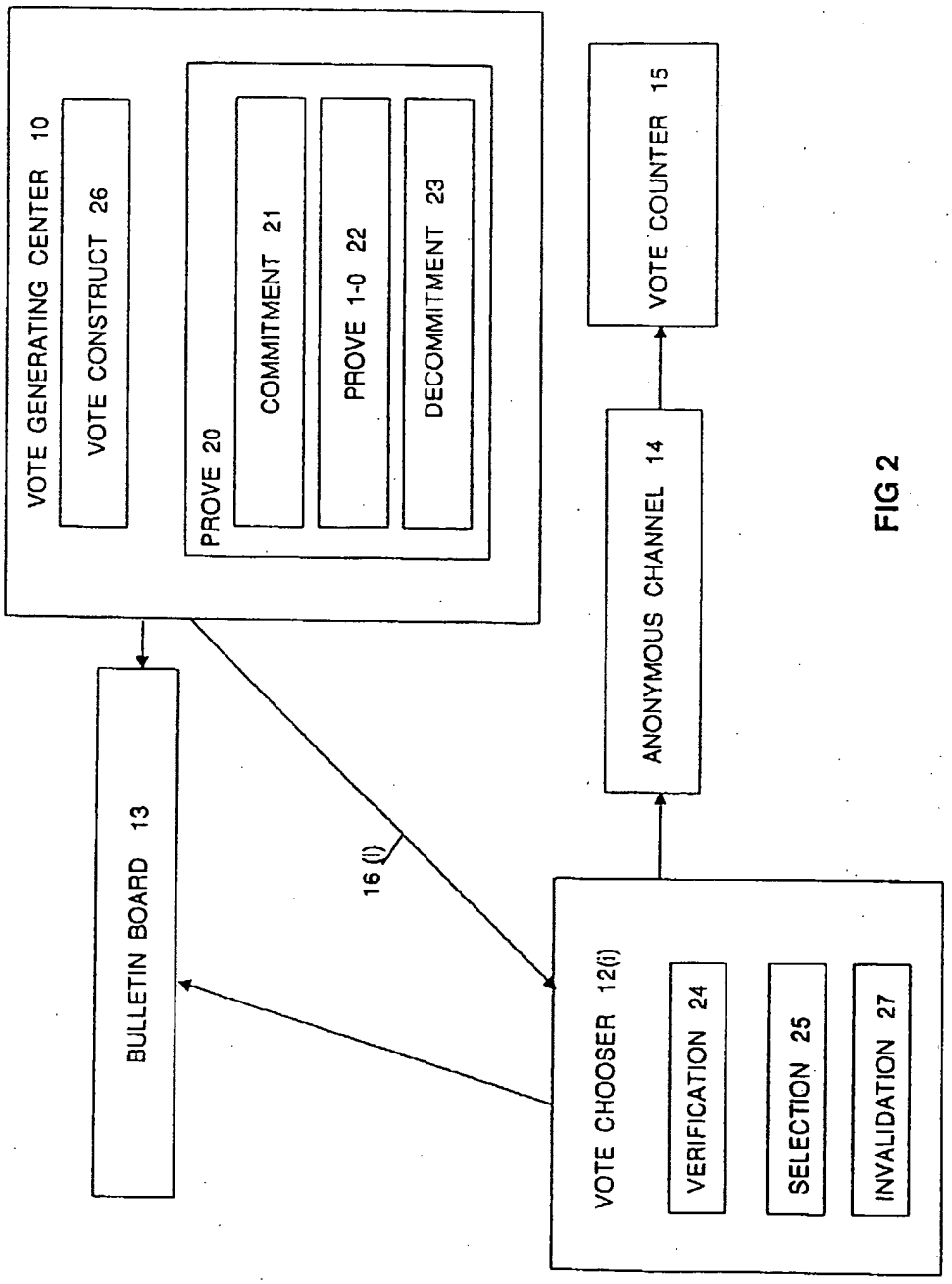

VOTE GENERATING CENTER 10
VOTE CONSTRUCT 26
PROVE 20
COMMITMENT 21
PROVE 1-0 22
DECOMMITMENT 23
VOTE COUNTER 15
ANONYMOUS CHANNEL 14
BULLETIN BOARD 13
16 (i)
VOTE CHOOSER 12(i)
VERIFICATION 24
SELECTION 25
INVALIDATION 27

FIG 2

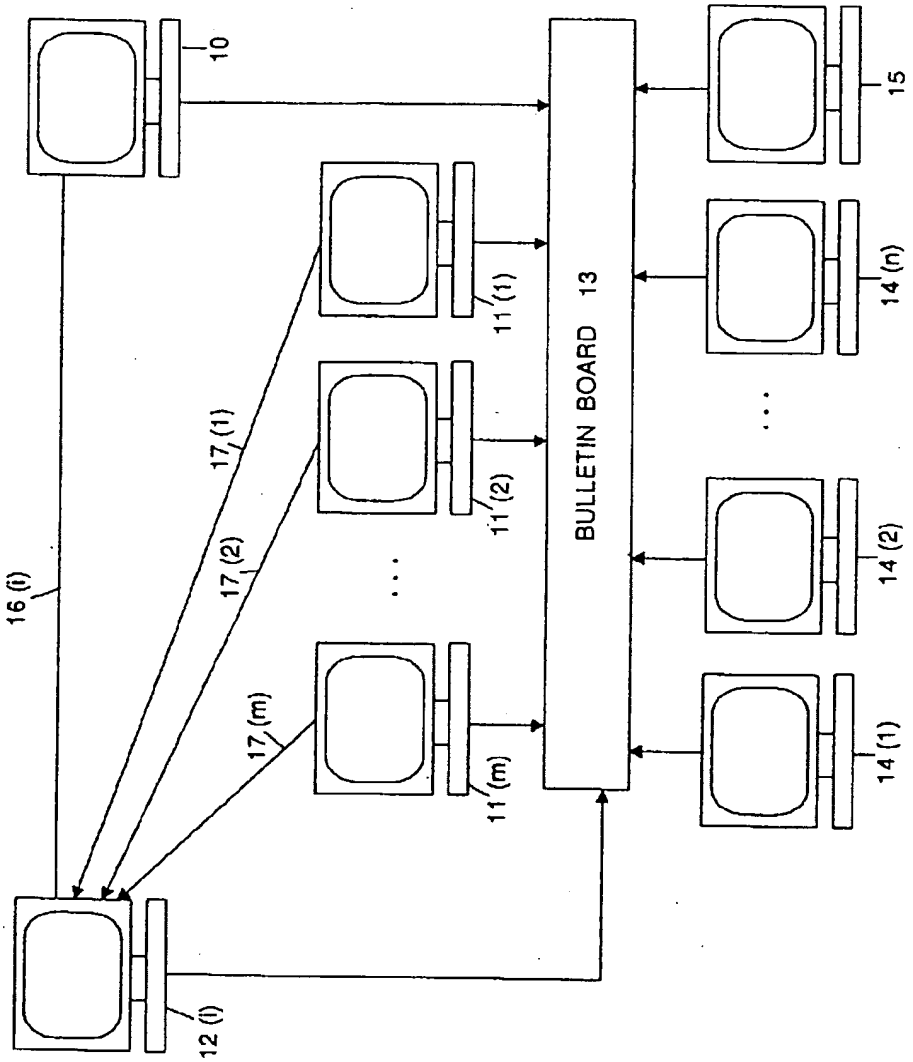

10
15
11 (1)
14 (n)
17 (1)
BULLETIN BOARD 13
11 (2)
14 (2)
16 (i)
17 (2)
17 (m)
11 (m)
14 (1)
12 (l)

FIG 3

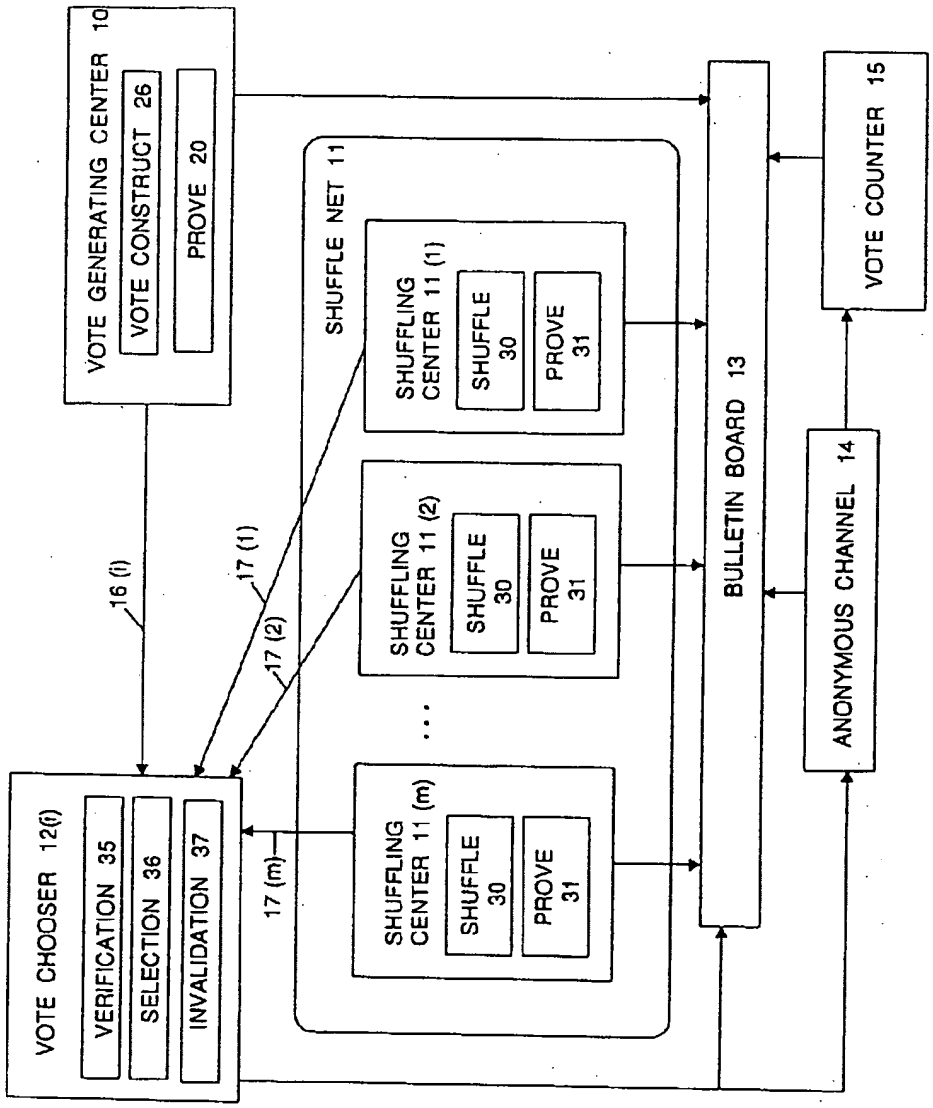

VOTE GENERATING CENTER 10
VOTE CONSTRUCT 26
PROVE 20
SHUFFLE NET 11
SHUFFLING CENTER 11 (1)
SHUFFLE 30
PROVE 31
SHUFFLING CENTER 11 (2)
SHUFFLE 30
PROVE 31
SHUFFLING CENTER 11 (m)
SHUFFLE 30
PROVE 31
BULLETIN BOARD 13
VOTE COUNTER 15
ANONYMOUS CHANNEL 14
VOTE CHOOSER 12(l)
VERIFICATION 35
SELECTION 36
INVALIDATION 37
16 (l)
17 (1)
17 (2)
17 (m)

FIG 4

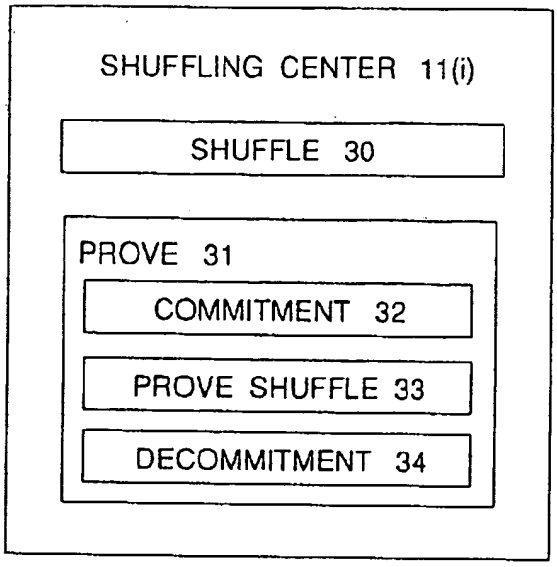


FIG 5

1. Abstract

A number-theoretic based algorithm provides for secure receipt-free voting. A vote generating center generates a choice of votes for each voter or vote chooser. The votes are encrypted, shuffled, and conveyed to a vote chooser along with information regarding how the votes were shuffled without being intercepted en route. The information is preferably sent along untappable secure channels. The method can incorporate validification of generation and shuffling of the votes using chameleon commitment and interactive proofs. The invention can be realized by current-generation personal computers with untappable channels and access to an electronic bulletin board.

2. Representative Drawing

FIG 1